UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/492,273	01/27/2000	Wolfgang Rankl	JEK/Rankl	9676

7590 10/06/2003

J. Ernest Kenney
Bacon & Thomas PLLC
625 Slaters Lane
4th Floor
Alexandria, VA 22314-1176

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	6

DATE MAILED: 10/06/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/492,273	RANKL, WOLFGANG	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-9 are pending.

2. The preliminary amendment of 1/17/2000 was received and considered.

Priority

3. Acknowledgment is made of applicant's claim for priority under 35 U.S.C. 119(a)-(d) based upon an application filed in Germany on 1/25/1999. A claim for priority under 35 U.S.C. 119(a)-(d) cannot be based on said application, since the United States application was filed more than twelve months thereafter.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 2 and 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

A broad range or limitation together with a narrow range or limitation that falls within the broad range or limitation (in the same claim) is considered indefinite, since the resulting claim does not clearly set forth the metes and bounds of the patent protection desired. Note the explanation given by the Board of Patent Appeals and Interferences in *Ex parte Wu*, 10

USPQ2d 2031, 2033 (Bd. Pat. App. & Inter. 1989), as to where broad language is followed by "such as" ("in particular") and then narrow language. The Board stated that this can render a claim indefinite by raising a question or doubt as to whether the feature introduced by such language is (a) merely exemplary of the remainder of the claim, and therefore not required, or (b) a required feature of the claims. Note also, for example, the decisions of *Ex parte Steigewald*, 131 USPQ 74 (Bd. App. 1961); *Ex parte Hall*, 83 USPQ 38 (Bd. App. 1948); and *Ex parte Hasche*, 86 USPQ 481 (Bd. App. 1949). In the present instance, claim 2 recites the broad recitation "an individual identifier", and the claim also recites "a serial number" which is the narrower statement of the range/limitation. Claim 8 is rejected by a similar rationale, again for the use of the phrase "in particular".

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1 and 3-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 4,200,770 to Hellman et al. (Hellman) in view of U.S. Patent 6,038,551 to Barlow et al. (Barlow).

Regarding claims 1 and 3, Hellman discloses a system wherein two conversers communicate over an insecure channel in substantially the same method as described in the

claim (see col. 3, lines 41-68, col. 4, lines 1-67 and col. 5, lines 1-3). This is commonly referred to in the art as the Diffie-Hellman key-exchange algorithm. Hellman's system discloses enabling "conversers" to communicate securely even if an unauthorized party intercepts all communication between them (see col. 2, lines 5-13), but lacks application of the algorithm to a chip card and a processing station. Barlow teaches that problems that exist with card-like mechanisms, such as lack of scalability, the difficulty in having to configure millions of devices with unique keys and the replacement of keys after the manufacture of the device, can be overcome by using customizable cards that are not bound to specific encryption keys (see col. 2, lines 17-66). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply Hellman's key-exchange algorithm to a smartcard system, eliminating the need to preprogram the hardware of the smartcard with specific keys, as taught by Barlow.

Regarding claims 4-5, Hellman discloses using modular exponentiation to determine the values to be sent from each converse and to determine the secret key (see col. 4, lines 18-67).

Regarding claim 6, Hellman discloses that the key sources may be random number generators (see col. 4, lines 1-5).

Regarding claim 7, Hellman discloses that the secure key generators generate keys that may be used in cryptographic devices (see col. 5, lines 1-3), used for enciphering and deciphering information.

Regarding claim 8, Hellman's system, as modified above, lacks transmission of additional keys to the card. Barlow teaches that to support multiple applications, the card must enable a user to transport keys from one application to another (see col. 4, lines 34-49).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Hellman's system to allow multiple keys to be transported through the medium secured by the algorithm (as taught by Hellman), enabling the supporting of multiple applications, as taught by Barlow.

8. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Barlow as applied to claim 1 above, and further in view of "Cryptographic Identification Methods for Smart Cards in the Process of Standardization" by Hans-Peter Königs. Hellman discloses a system, as modified above, but lacks using an individual identifier to generate the initial value for the card. Königs teaches that one can greatly simplify the problem of key management and make an explicit public key unnecessary (see page 46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Hellman's system to use identification information as the basis for a key, gaining the benefit of simplified key management, as taught by Königs.

9. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Barlow as applied to claim 8 above, and further in view of U.S. Patent 5,224,163 to Gasser et al. (Gasser). Hellman's system, as modified above, lacks removal of the original session key after the receipt of personalization information. Gasser teaches that removing a key after it's use in an authorization system ensures security even if one of the participants is compromised thereafter (see col. 15, lines 51-65). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to remove the session key from

Hellman's system, as modified above, after the initial transaction was complete to prevent compromise of both the card and the apparatus if either was compromised, as taught by Gasser.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:30 p.m.. The examiner can also be reached on alternate Fridays from 8:00 a.m. – 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

MJS
29 September 26, 2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100